

## UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE ACCOUNT  
Todd michael5822@gmail.com THAT IS STORED AT  
PREMISES CONTROLLED BY GOOGLE INC.

Case No.

1:17mj256

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
SEE ATTACHMENT A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

Items constituting the evidence, contraband, fruits or instrumentalities of violations of 18 U.S.C. § 1030(a)(7)(A) and (c)(3)(A), Threatening to damage a protected computer, 18 U.S.C. § 875(b), Interstate communicating threats to persons, and 18 U.S.C. § 875(d), Interstate threats, as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

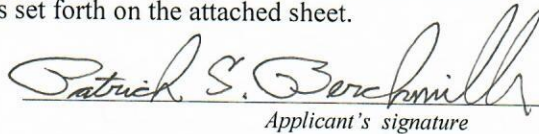
- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1030(a)(7)(A),(c)(3)(A)	Threatening to damage a protected computer
18 U.S.C. § 875(b), (d)	Interstate communicating threats to persons, Interstate threats

The application is based on these facts:  
(SEE ATTACHED AFFIDAVIT)

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Patrick S. Berckmiller, Special Agent  
Printed name and title

Sworn to before me and signed in my presence.

Date:

08/04/17

  
Judge's signature

City and state: Greensboro, North Carolina

The Honorable L. Patrick Auld, Magistrate Judge  
Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH  
OF INFORMATION ASSOCIATED  
WITH THE ACCOUNT  
**Toddmichael5822@gmail.com,**  
THAT IS STORED AT PREMISES  
CONTROLLED BY GOOGLE INC.

Case No. 1:17-mj-256

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

1. I, Patrick S. Berckmiller, being first duly sworn, hereby depose  
and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and has been so employed since November 1998. Since April 2016, affiant has been assigned to investigate cyber related crimes to include fraud and related activity in connection with computers. From March 1999, until April 2016, affiant was assigned to investigate foreign counterintelligence matters and theft of trade secrets crimes. Affiant received training from the FBI regarding cybercrimes, foreign counterintelligence, and theft of trade secrets, and has previously been involved in investigations involving espionage, export violations, bank robbery, kidnapping, fugitives from justice, white collar crimes, and computer crimes involving the theft of proprietary data.



Most recently, I have been involved in an investigation regarding a cyber extortion matter. As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1030(a)(7)(A) and (c)(3)(A), Threatening to damage a protected computer, 18 U.S.C. § 875(b), Interstate communicating threats to persons, and 18 U.S.C. § 875(d), Interstate threats (hereinafter, the “TARGET OFFENSES”) have been committed by Todd Michael GORI. A grand jury in the Middle District of North Carolina returned a four-count indictment on April 25, 2017, charging the aforementioned offenses in case number 1:17CR146-1, *United States v. Todd Michael Gori*. There is also probable cause to search the information described in Attachment A for evidence of the TARGET OFFENSES, as described in Attachment B.

5. I make this affidavit in support of an application for a search warrant for information associated with one e-mail account that is stored at premises controlled by Google Inc., an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Middle District of North Carolina is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

7. This affidavit proceeds as follows. In this section, I outline the factual allegations in support of a warrant to search one email account.



8. On or about April 18, 2016, Federal Bureau of Investigation Special Agent Patrick Berckmiller learned of a cyber extortion threat against TSI Healthcare, 101 Europa Drive, Suite 200, Chapel Hill, North Carolina, 27511 website: [www.tsihealthcare.com](http://www.tsihealthcare.com), Facebook: TSI Healthcare. The following message (quoted verbatim including typographical errors) was sent through the TSI Healthcare website's "contact us" page:

-----Original Message----- From: Todd Gori [mailto:[toddmichael5822@gmail.com](mailto:toddmichael5822@gmail.com)] Sent: Monday, April 18, 2016 10:04 AM To: Info <[info@tsihealthcare.com](mailto:info@tsihealthcare.com)> Subject: Contact Us Page Inquiry Someone has filled out the contact us form on our contact page. Below is their information: Name: Todd Gori Practice Name: Cheryl Patterson City: Wenatchee State: Washington Email: [toddmichael5822@gmail.com](mailto:toddmichael5822@gmail.com) Phone Number: 7027010985 How Did You Hear About Us: TSI Healthcare Called Me Message Body: hello, This is cheryl thompsons son. I am giving you, TSI healthcare two choices. You either lay-off my crazy workaholic mother Cheryl Thompson and replace her with me, an operator 100x better that she is oppressing. Or I will take out your entire company along with my comrades via a cyber attack. Again you have two choices. Get ride of her and hire me. Or slowly be chipped away at until you are gone. She is a horrible operator that can only manage 2 screens with an over inflated travel budget. I fly at least 10x as many places as this loon on 1/5th of the budget.

I have petitioned for a job with you guys with her as a reference as I am a felon with computer skills and need assistance getting work as technically I have "no work history". She declines everytime and burries me even further. I even stated this straight from TSI website "Center for Generational Kinetics Best Places to Work for Millennials Top 75 Millennial Employer in the U.S. 2015" and she shunned me like I was some type of idiot. How rude of my mother. A son that has wanted to be her friend both on facebook and in real life. Most people want to run from there parents in the other direction I am trying to be this woman's friend and help here and she is busy making me cry daily and making someone with good computer skills much better then her homeless and starving. I'm giving you guys 72 hours to respond until the attack goes full scale. There is nothing that can be done to stop the attacks. I

have ran multiple penetration tests on your entire network and your company fails miserably. Again let me be clear. The only way I will work with TSI and stop the attack is to fire Cheryl Thompson (my crazy workaholic mother) and hire me and ensure I am compensated enough to keep her well sedated and normal inside a nursing home before she destroys her son like she destroyed 4 families. This is not a threat this is not a means of leverage this is saving myself and my mother and if you do not comply you can prepare for the most annoying and pesky uphill cyber battle your company has ever seen. She will also be blocked from working while the attack is taking place. If it has to take place in it's entirety as it has already begun.

9. On April 21, 2016, a Special Agent with the Federal Bureau of Investigation (FBI) along with a Detective from the Wenatchee Police Department, located GORI in Wenatchee, Washington. After informing GORI of the identity of the interviewing agent and the nature of the interview, GORI demanded an attorney. GORI then stated that he did not wish to talk and slammed the apartment door. The interviewing agent tried again to talk with GORI when GORI emerged from the apartment a short time later. GORI asked to see the investigating agent's credentials. The investigating agent showed GORI the credentials. Gori stated that he wanted to photograph the credentials and ran back into the apartment to retrieve his cell phone. The investigating agent would not allow GORI to take a picture of the credentials per FBI policy, and the attempted interview was concluded. A strong odor consistent with marijuana was emanating from GORI's apartment.



10. On May 2, 2016, the FBI received reports from the Master Call Record of the Wenatchee Police Department (WPD), Wenatchee, Washington. A call to the WPD on February 18, 2015 identified a Todd Michael GORI, date of birth February 4, 1989, as using telephone number 702-701-0985. A call to the WPD on 01/01/2016 identified a Todd Michael GORI, date of birth February 4, 1989, using telephone number 702-701-0985. A call to the WPD on March 12, 2016, identified a Todd Michael GORI, using telephone number 702-701-0985. A call to the WPD on March 15, 2016, identified a Todd Michael GORI, date of birth February 4, 1989, as using telephone number 702-701-0985.

11. On March 1, 2017, TSI Healthcare received a phone call from an individual who identified himself as Todd GORI. That phone call reached a TSI Healthcare employee who recalled taking a prior call from GORI either earlier that month or in a month recently preceding the March 1, 2017, call. In the prior call, GORI began by stating something like. "It's Todd, I'm your worst nightmare," before asking the TSI employee to contact GORI'S mother. When the TSI employee replied that she would do her best to get the message to GORI'S mother, GORI said that no one puts him through to her and he is

down to his last \$1,200.00. He said if he had to, he will buy a plane ticket and fly to North Carolina, go to a gun show, purchase a gun and come to the office and begin shooting the place up, even though he hates flying. The TSI employee recognized the following two telephone numbers being used by GORI, 509-662-8165 and 702-701-0985, when he called into TSI Healthcare. The TSI employee believes she has spoken to GORI on 10-20 occasions. As a result, TSI Healthcare felt this was a credible threat and called 911 to file a police report with the Chapel Hill Police Department, who notified the FBI.

12. On March 1, 2017, the FBI contacted the Wenatchee Police Department (WPD), Wenatchee, Washington. The WPD located GORI at his place of employment, Office Depot, and approached him in regards to making computer threats to a clinic in S. Carolina (sic). GORI said he wasn't going to make any statements about that for legal reasons. The officers told GORI not to communicate with target of the threats anymore. On the same day, the Chapel Hill Police Department, Criminal Investigations Division published a law enforcement notice to Be On the Look Out (BOLO) for Todd GORI in regards to these threats.

13. On March 30, 2017, Special Agent Berckmiller was made aware of the following additional emails which were sent to a TSI Healthcare



employee from the user of email account toddmichael5822@gmail.com (shown below verbatim including typographical errors):

From: Todd Michael  
<toddmichael5822@gmail.com<mailto:toddmichael5822@gmail.com>>  
Date: March 30, 2017 at 8:54:27 PM MST  
To: David Dickson Jr.  
<ddickson@tsihealthcare.com<mailto:ddickson@tsihealthcare.com>>  
Subject: Re:

a hint would be 2-5m plus benifits that should last us until we die. otherwise i am shutting you down david. i want my mother back.

On Thu, Mar 30, 2017 at 8:51 PM, Todd Michael  
<toddmichael5822@gmail.com<mailto:toddmichael5822@gmail.com>> wrote:  
the only way for you to stop this is to terminate my mother tomorrow with adequate compansation. no two weeks. no grace period. just terminate her and structure a comp package / check that will ensure i make it to my eath window 50-60 and she will die off peacefully with decent life.

otherwise i am shutting your company down quickly piece by piece tomorrow by dusk and there is not a damn thing your corrupt ass or your crooked as friends in the feds can do.

On Thu, Mar 30, 2017 at 8:48 PM, Todd Michael  
<toddmichael5822@gmail.com<mailto:toddmichael5822@gmail.com>> wrote:  
i tried to be a regular person to you and all the others. instead you assholes call the feds on me twice. instead you assholes have local PD show up to my work nearly getting me fired.

you people stole my mothers soul. my real mother. and you are stealing pieces of mine. i sent a more detailed email to info@tsihealthcare.

if my möther is not terminated tomorrow with a generous package to ensure we are both well enough off to live the rest of our short lives (ill be lucky to

live to 50 given family health issues) then you can fully expect your company to undergo serious digital issues and be very lucky to even have a digital precense online

you can call the feds all you like liek the rat you and your people are there is nothing they or you can do now.

i sit on a roof contemplating suicide tonight (again) and my own mother talks endless shit to me. Not my old mother. The new one. The one you people created. The one you people stole the soul from. The soul you are stealing from me through her.

i dont care what you think about my emails. How crazy i am. FBI or whatever. I really dont care david. If my mother is terminated without adequate compensation it will make matters even worse.

You must understand this is not an extortion attempt or a terrorist plot (nobody likes to feel powerless and extorted esp by some punk behind a pc). This is me saving my mother, myself, and what little family i have left. After you people got involved my entire family has been shattered to bits.

please ensure my mother is terminated tomorrow with adequate compensation. its the only way to stop the attack. Immediate termination with generous comp package for her services and selling her fucking soul to you people.

if i am not taken care of along with her in the compensation package then i can guarantee you pending a nuclear exlosion on all continents you epeople will be working and buidling your company from all paper. you will be lucky if i let you even have a website or send a single email.

again let me make it clear to you and your corrupt friends at the FBI. I have no interest in doing this. But you epeople stole my real mother from me. Make it right or i will make it right by serviging justice against the corrupt (you and your other corrupt friends that run in vast numbers internationally)



14. On March 31, 2017, GORI made two calls to TSI Healthcare, stating he wanted to reach his mother, Cheryl Thompson. In the second call which GORI made to TSI Healthcare, he began to provide a TSI Healthcare staff member his contact information, which began with "toddmichael" and then became inaudible.

15. On April 3, 2017, GORI called TSI Healthcare and told a TSI Healthcare staff member that he wants his mother to call him on Mexican telephone number 011-52-998-883-0270.

16. On April 6, 2017, Todd GORI posted the following messages on his Facebook page:

April 6 at 11:25pm

FEDS TROLLIN HARD THATS ALL THEY  
KNOW #FAGGOTS

April 6 at 11:27pm

FEDS = 0 SKILL ALL TROLLS

April 6 at 11:26pm ·

99.9% OF FEDS ARE FLAMING  
COCKSUCKING CLOSETED  
HOMOSEXXUALS. REMEMBER THAT

17. On April 12, 2017, GORI called TSI Healthcare, stating that he was in Mexico and his mother was able to scrape together \$100.00. GORI further stated he has emails waiting from his mother, and asked TSI Healthcare staff to have his mother check her emails. He provided a call-back telephone number of 702-701-0985. GORI stated that because he was using GoogleVoice, his phone reception for incoming calls was spotty.

18. On April 13, 2017, GORI called TSI Healthcare from "his other number" (no further information), and left a message asking to please get a message to his mother and that he was still waiting on emails back from her.

19. On June 19, 2017, GORI was taken into custody by United States Customs and Border Protection (CBP) Officers, upon his arrival at Dallas Fort Worth International Airport, Texas, from Cancun, Mexico. GORI's arrest was pursuant to the federal arrest warrant in Middle District of North Carolina case 1:17CR146-1. A CBP Officer spoke to GORI in the normal course of processing upon arrest. When the officer asked GORI how long he had been in Mexico, GORI said he had been in Mexico for about three months, and was trying to establish residency there. The officer relayed this information to an FBI Special Agent later that day in person. At the time of his arrest, GORI was in possession of the following items: one black SanDisk Cruzer Glide 16GB Thumb drive, one black SanDisk Cruzer Glide 16GB



Thumb drive, one black Dell 8GB Thumb drive, one black Digipower card reader Thumb drive, one black Unirex 8GB Micro SD card, one black Toshiba 2TB External Hard drive serial Number 64EBTQAOT18B, one black Alcatel Smart Phone, model #5027B, MEID DEC: 089712410303605589, MEID HEX: 35790707370455, one white Dell Inspiron P24T laptop computer serial number F9ZFD82, one gray Alienware P42F laptop computer serial number 2RT4M72, one black Toshiba 1TB external hard drive serial number 74EZX6XFSTT1, one gray Samsung SM-G357M Smart Phone serial number R28F90EEZXL with number 9983948587 taped on the back, one black Seagate expansion desktop 8TB hard drive serial number NA8FCKJX, one black Seagate expansion desktop 8TB hard drive serial number NA8FCHBL, one black ASUS RT-N12 Wireless N Router serial number E7IADQ002112.

### **BACKGROUND CONCERNING E-MAIL**

20. In general, an e-mail that is sent to a Google Inc. subscriber is stored in the subscriber's "mail box" on Google Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google Inc. servers indefinitely. Even if the

subscriber deletes the e-mail, it may continue to be available on Google Inc.'s servers for a certain period of time.

21. In my training and experience, I have learned that Google Inc. provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google Inc. allows subscribers to obtain e-mail accounts at the domain name @gmail.com, such as the e-mail account[s] listed in Attachment A. Subscribers obtain an account by registering with Google Inc. During the registration process, Google Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google Inc. subscribers) and information concerning subscribers and their use of Google Inc. services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. A Google Inc. subscriber can also store with the provider files in addition to e-mails, such as address books, Google Hangouts, contact or buddy lists, calendar data, chat history, pictures via a linked Google Photos account (other than ones attached to e-mails), bookmarks, and other files such as those stored in linked Google Documents and Google Drive



applications, on servers maintained and/or owned by Google Inc. Google Inc. also stores search terms entered into Google Search tool by a user who is simultaneously logged into their Google e-mail account. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures, files, and search terms.

23. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone number(s) and other identifiers, alternative e-mail addresses, and, for paying subscribers, any means and sources of payment to include any credit or bank account number. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user(s).

24. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the

account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

25. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

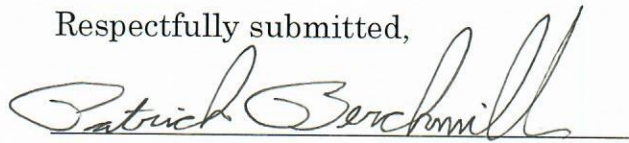
### **CONCLUSION**

26. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google Inc. who will then compile the requested records at a time convenient to it, there



exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Patrick S. Berckmiller  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on August 4,  
2017



THE HONORABLE L. PATRICK AULD  
UNITED STATES MAGISTRATE JUDGE  
MIDDLE DISTRICT OF NORTH CAROLINA

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to records associated with all Google services for the account listed below, in the form of e-mail, chat communications, search history, contacts, calendar entries, Google Drive documents, Google Hangouts, bookmarks, and Google Photo Albums, which are stored at premises controlled by Google Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California, 94043 and electronic legal process via the Google Law Enforcement Response System (LERS) at <https://www.lers.google>:

- Toddmichael5822@gmail.com



## ATTACHMENT B

### Particular Things to be Seized

#### I. Information to be disclosed by Google Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, in the form of emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period 04/01/2016 – 06/19/2017:

a. The contents of all e-mails associated with the account, in the form of stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, originating IP information for all e-mails sent from the account, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates,

account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, in the form of address books, contact and buddy lists, calendar data, pictures, search history, Google Chat history, Google Documents files, Google Drive files, bookmarks, Picasa Albums and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.



## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of 18 U.S.C. § 1030(a)(7)(A) and (c)(3)(A), Threatening to damage a protected computer, 18 U.S.C. § 875 (b), Interstate communicating threats to persons, and 18 U.S.C. § 875(d), Interstate threats, for each account or identifier listed on Attachment A, in the form of:

- a. Any form of communication directly or indirectly involving TSI Healthcare;
- b. Threats in the form of documents, emails, voice recordings, texts, photos, images, scans;
- c. Information referencing employees of TSI Healthcare, (including names, addresses, phone numbers, email addresses, or any other identifying information);
- d. Photographs, images, building plans, maps, directions, web browsing history, search engine data, or identifying information regarding the TSI Healthcare facility.
- e. Information regarding the TSI Healthcare's website, webportal, employee log in portal, Facebook page, or other social media accounts.
- f. Hacking tools, malware, ransomware, Denial of Service (DoS), Distributed Denial of Service (DDOS) software or services or discussion of such tools that can be used in order to gain unauthorized access or deny access to a protected computer.

- g. Manifesto, or any other document relating to the use or desire of violence directed at others.
- h. Any information related to the research, planning, purchase, preparation or use of firearms in the commission of an act of violence.
- i. Any information relating to acquiring firearms at gun shows.
- j. Records of who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.



**CERTIFICATE OF AUTHENTICITY OF  
DOMESTIC BUSINESS RECORDS PURSUANT  
TO FEDERAL RULE OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google Inc., and my official title is \_\_\_\_\_.

I am a custodian of records for Google Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google Inc., and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google Inc.; and
- c. such records were made by Google Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature